April 14, 2016 Volume 9, Issue 7

Blue Top Newsletter

Upcoming Meetings and Training

Meeting/Training	Date & Time (EST)	Location	Dial-In Info
Registrar Refresher Training	Thu, Apr 14 2:30 to 3:30	Telecon/Webinar	888-455-1864 Passcode: 3611044
CAB	Wed, May 4 9:00 to 12:00	GSA Central Office 1800 F St. NW Room 3042	No telecon provided
User Group	Wed, May 11 9:00 to 12:00	GSA Central Office 1800 F St NW Room 6004	888-455-1864 Passcode: 5887966
Registrar Classroom Training	Wed and Thu Apr 20-21 May 18-19 Jun 15-16	HPE Chantilly, VA	Contact Jim Schoening for information or to Register

Light Credentialing Solution (LCS) workstations must have v4.0 or v4.0.1 installed by April 23 due to infrastructure maintenance; v4.0.1 available

The USAccess team will upgrade the USAccess F5 Edge server on April 23rd. The F5 is used by LCS kits to connect to the USAccess service and complete enrollments. Connections are made by clicking on a desktop icon (labeled F5) located on LCS machines.

The April 23rd work requires all LCS machines to have an updated F5 desktop client that is included in both the Light v4.0 and v4.0.1 installers. The 4.0.1 installer is now posted on the USAccess SFTP server. If an LCS does not have the updated F5 client following April 23, the kit won't be able to complete enrollments. **As a result, all LCS machines must be updated to v4.0 or v4.0.1 by April 23rd.**

The new F5 configuration also allows enrollment connections using the TLS 1.2 protocol with stronger (256 bit) ciphers. Currently it only supports TLS 1.0 and TLS 1.1. Once Light 4.0 or 4.0.1 is installed and the F5 work completed on April 23, Agencies with networks configured for TLS 1.2 will no longer need to uncheck the TLS 1.2 checkbox in Internet Explorer to connect to Assured Identity/complete enrollments. Agencies can also continue to use 1.0 and 1.1 if they wish to.

Special Points of Note:

Now found on www.fedidcard.gov:

- **Service Order Requests and Test Card Orders**
- **Role Holder Web Based Training Registration**
- **Deployment Activities and USAccess Center Status Alerts**
- **Contact Sharon Meng (Sharon.Meng@gsa.gov) to be added to USAccess distribution lists.**
- **Contact Jim Schoening (jim.schoening@gsa.gov) for Registrar Classroom Training sign up**

Inside this issue:

How to get the updated installers
The Light v4.0.1 installer (and updated guides) is posted on the SFTP server. An email was sent on Tuesday, March 29 to Agency Leads announcing the availability of v4.0.1 which includes fixes to several known issues with v4.0. A release notice for v4.0.1 is also posted on the Agency Lead portal. If you cannot remember your login to the SFTP server, please contact the MSO at hspd12@gsa.gov.

Issue with checking in cards via the Credential Inventory Tool

Last week (Wednesday through Friday, April 6-April 8), the card production facility had connectivity issues with their carrier. As a result, the USAccess service did not receive card batch files from the CPF during this outage period. This prevented Activators from checking cards in via the Credential Inventory Tool or activating new cards, even though card shipments were received.

The CPF service was restored Friday afternoon, and the backlog of card batch files were processed and cards could be checked in and activated by late Friday. Advisories were posted on TRACKS throughout the outage. We appreciate your patience as we worked with our CPF to resolve the issue.

NIST Releases SP 800-85A-4, PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-4 Compliance)

The National Institute of Standards and Technology released Special Publication (SP) 800-85A-4, PIV Card Application and Middleware Interface Test Guidelines on April 12. SP 800-85A-4 provides derived test requirements and test assertions for testing PIV Middleware and PIV Card Applications for conformance to specifications in SP 800-73-4, Interfaces for Personal Identity Verification, and SP 800-78-4, Cryptographic Algorithms and Key Sizes for Personal Identity Verification. The document has been updated to include additional tests necessary to test the new features added to the PIV Data Model and card interface as well as to the PIV Middleware in SP 800-73-4 Parts 1, 2, and 3.

These include:

- Tests for retrieving newly added optional PIV data objects such as the Biometric Information Templates Group Template data object, the Pairing Code Reference Data Container and the Secure Messaging Certificate Signer data object;
- Tests for populating these newly added data objects in the PIV Card Application;
- Tests to verify the on-card biometric comparison mechanism;
- Tests to verify the correct behavior of secure messaging and the virtual contact interface; and
- Tests to verify that the PIV Card Application enforces PIN length and format requirements.

NIST’s SP 800 series publications are available at: http://csrc.nist.gov/publications/PubsSPs.html

Release 9.9 Known Issues Log

A USAccess Software Release 9.9/Light Installers 4.0 Known Issues document is posted on the ALP. This document lists known issues following these releases, their user impact and the workaround until a fix is available. This document was updated last week so be sure to review to be informed on when fixes were pushed to production.

Updated Training Guides

The MSO has recently published new a Fingerprint Submission Guide and updated two other guides.

Fingerprint Submission to OPM 2016 04 05 – available on ALP
This guide is intended for Adjudicators. It contains information about the process for submitting and resubmitting fingerprint packages to OPM. OPM contributed to this document by providing definitions of the Transaction Type options, and clarity on the resubmission process. There has been confusion in the past about the proper Transaction Type to select and about the resubmission process, so we hope your Adjudicators find this information helpful.

PCA Guide v1.2 April 2016 – available on TRACKS and ALP
The PCA Guide has been updated to reflect the changes made available in Light installer v.4.0.1. The software updates addressed in this guide are:

- Re-labelled "Affiliation" field to "Email" field on the Applicant Validation Screen
- Resolved issue with completing PIN changes when conducting card updates

Guidance on resetting UPN Password on Fixed Workstationsv2 – available on TRACKS and ALP
Updated guidance based on Registrar/Activator feedback. The content and formatting have been updated with the intention of making the process easier to understand and complete.

Service Enhancements

Changes/updates since last Blue Top

- Light Installers v4.0.1 were posted on March 29.
- Maintenance completed as scheduled on March 26.
- A fix was pushed on March 24 for a known issue with the ASR supplemental report (fallout from Release 9.9). Please see the updated Release 9.9 Known Issues list posted on the Agency Lead Portal.
- Modified Zone 17 for Department of State Office of the Inspector General
- Onboarded Federal Retirement Thrift Investment Board

Planned changes

For any maintenance downtime periods, please schedule some buffer time to resume enrollment and activation appointments to account for any unanticipated delays in service.

- April 23. Maintenance is scheduled for this Saturday to update the F5 server. See the previous article on the impact for LCS kits due to this change. The USAccess service and portals will be unavailable for most of the day.
- April 30. Routine maintenance is scheduled on this Saturday and the USAccess service and portals will be unavailable for most of the day.

Security Tip

No matter how much expertise and money your agency puts into securing its network and data assets—firewalls, security appliances, encryption, etc.—the human component of the security system is the most critical and quite often the most vulnerable. Social Engineering and Phishing are two techniques employed to attack the human component.

Social Engineering

Social Engineering is the manipulation of words and/or actions that are intended to establish a false sense of trust and confidence. Once trust is established, the attacker's objective is to ultimately induce a desirable response. When an unsolicited contact is asking for information, consider whether the person you're talking to deserves the information they're requesting and how the information may be employed by an attacker.

Social engineers have repeatedly shown that those who focus on technology alone to solve the problem of protecting an IT system and its data are addressing only part of the problem. They discount or ignore the evidence that the human component will always be the weakest link. Technology is important but minimizing the vulnerability of this weak link is the system user's responsibility.

Successful social engineering often depends on pressuring the target and not allowing time to think about their decision. If you find yourself dealing with someone and suddenly you feel pressured to make a decision, or to take some immediate action, you should stop and ask yourself; where is this pressure coming from - internal or external - and why am I being pressured? Unwarranted pressure is a big red flag and it should set off your alarm bells. Be wary if the contact does not match the person or message. A good personal policy is that when something doesn't seem right it isn't. Trust your gut instincts.

Phishing

Phishing attacks are closely related to social engineering and refer to the process where someone posing as a legitimate contact contacts you by email, telephone or in person. The purpose is to lure you into providing sensitive information. The information requested may then be used to access your user account, another user's account or agency assets.

Email phishing attacks will often include eye-catching or attention-grabbing statements. These attacks are designed to immediately get your attention. Phishing scams are wide and varied and typically include information request from someone claiming to have a legitimate authority. Communications that unexpectantly appear in you inbox from a senior agency manager that you do not typically deal with directly is a red flag. You may recognize the source – your agency's CIO office or IT Security Office, but the name is one that you do not recognize. Unless you are sure, you should not respond. If you are not sure, report it.
Many people will fall prey to social engineering or phishing attacks because the attackers understand human nature. These are sophisticated people that leverage this understanding to exploit human nature and our desire to be helpful and accommodating. Remember, attackers are skilled at establishing trust and then inducing a desired response.

Protecting yourself and your agency is not rude or hard-hearted. It is prudent. If there is any doubt STOP and contact your ISSO or agency help desk and report it.

The following are small samplings of techniques that are employed by attackers. These may not appear to be directly applicable to a government user but with simple variations, these techniques can, and are, successfully employed by an attacker. Our defense begins with the understanding that we are all targets.

The basic rule is: when in doubt, don't!

Technique	Description
Social Engineering or Phone Phishing	This technique uses the manipulation of words and/or actions intended to establish a false sense of trust and confidence. Once the trust is established, the attacker's objective is to induce a desirable response. When you receive an unsolicited contact that is asking for agency or personal information, consider whether the person actually deserves or needs the information they are requesting and how could the information be employed by an attacker.
Instant Messaging	An attacker may employ this helpful and convenient messaging application by sending an instant message with a link directing the user to a fake phishing website. The instant message may appear to be from someone you know and this link may have the same look and feel as the legitimate website. Never provide personal or agency specific information to unsolicited sites. If a message is unexpected, do not click on the link. Call the person and make sure.
Web Based Delivery	Web based delivery is a sophisticated phishing technique. It is also known as "man-in-the-middle" attack. For this technique the attacker is located in between the original legitimate website and the phishing system. The phisher can then trace details during a transaction between the legitimate website and the user. As a user continues to pass information, it will be gathered by the phishers, without the user knowing about it.
Link Manipulation	Link manipulation is another form of previously noted techniques where the phisher sends a link to a website. When the user clicks on the deceptive link, it opens up the phisher's website instead of the website mentioned in the link. A commonly used anti-phishing defense is to move the mouse over the link to view the actual address. If it looks strange, assume it is, and don't click on it.
Key Loggers	Key loggers refer to the malware used to capture inputs from the keyboard. Once captured the information will then be sent to an attacker who will decipher passwords and other sensitive information. Key loggers may be installed on your system by clicking on unfamiliar links or opening attachments sent by unreliable or unknown sources.

Explore the Government Acquisition Gateway Yet?

The Acquisition Gateway, otherwise known as the Common Acquisition Platform (CAP) and built by GSA, helps federal government buyers from all agencies act as one acquisition community. The Acquisition Gateway features information on government-wide contract vehicle comparisons, acquisition best practices, market research tools, prices paid data, and other useful tools and features. Federal employees with a PIV card or approved contractors can access the site. Sign up at https://hallways.cap.gsa.gov